AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for a probing entity to detect a duplicate IP address, the method comprising:

generating an identifying value that identifies a random period of time to wait before probing a network with which a probing entity desires to interact;

waiting a random period of time related to the identifying value;

sending one or more first ARP probes onto the network with which the probing entity desires to interact;

determining whether a response to the first ARP probes indicates that there is a duplicate IP address conflict;

determining whether the probing entity is connected to an active network, comprising:[[;]]

analyzing network traffic received by a network interface associated with the probing entity;

analyzing electrical signals received from hardware associated with the network with which the probing entity desires to interact; and

analyzing BPDUs (Bridge Protocol Data Units) received by a network device associated with the network with which the probing entity desires to interact;

sending one or more second ARP probes onto the network with which the probing entity desires to interact; and

determining whether a response to the second ARP probes indicates that there is a duplicate IP address conflict.

2. (Original) The method of claim 1, comprising:
sending ARP probes until the probing entity is connected to an active network.

3. (Previously presented) The method of claim 2, comprising:
not employing the potentially duplicate IP address until after all the processing associated with claim 2 has been completed.

4. (Previously presented) The method of claim 1, the length of the random period of time is generated by examining at least one of a GUID, a physical address, an IP address and a counter.

5. (Previously presented) The method of claim 1, the one or more first ARP probes contain the physical address of the probing entity and a potentially duplicate IP address.

6. (Previously presented) The method of claim 5, the response to the first ARP probes contain the physical address of the probing entity, the physical address of a responding entity, the IP address of a responding entity and the potentially duplicate IP address.

7. (Previously presented) The method of claim 6, determining whether a response to the first ARP probes indicates that there is a duplicate IP address conflict comprises comparing the potentially duplicate IP address of the response to the potentially duplicate IP address associated with the probing entity.

8. (Previously presented) The method of claim 7, the one or more second ARP probes contain the physical address of the probing entity and a potentially duplicate IP address.

9. (Previously presented) The method of claim 8, the response to the second ARP probes contain the physical address of the probing entity, the physical address of the responding entity, the IP address of the responding entity and the potentially duplicate IP address.

10. (Previously presented) The method of claim 9, determining whether a response to the second ARP probes indicates that there is a duplicate IP address conflict comprises comparing the potentially duplicate IP address of the response to the potentially duplicate IP address associated with the probing entity.

11. (Cancelled)

12. (Currently amended) A computer readable medium storing computer executable instructions operable to perform a method for a probing entity to detect a duplicate IP address, the method comprising:

generating an identifying value that identifies a random period of time to wait before probing a network with which a probing entity desires to interact;

waiting a random period of time related to the identifying value;

sending one or more first ARP probes onto the network with which the probing entity desires to interact;

determining whether a response to the first ARP probes indicates that there is a duplicate IP address conflict;

determining whether the probing entity is connected to an active network, comprising:[[;]]

analyzing network traffic received by a network interface associated with the probing entity;

analyzing electrical signals received from hardware associated with the network with which the probing entity desires to interact; and

analyzing BPDUs (Bridge Protocol Data Units) received by a network device associated with the network with which the probing entity desires to interact;

sending one or more second ARP probes onto the network with which the probing entity desires to interact; and

determining whether a response to the second ARP probes indicates that there is a duplicate IP address conflict.

13. (Previously presented) The computer readable medium of claim 12, the method further comprises:

sending ARP probes until the probing entity is connected to an active network.

14. (Previously presented) The computer readable medium of claim 13, the method further comprises:

not employing the potentially duplicate IP address until after all the processing associated with claim 13 has been completed.

15. (Currently amended) A system for detecting and preventing the use of duplicate IP addresses comprising:

a random time period generator operable to produce a value representing a period of time that a probing entity should wait before invoking the processing of a probe generator;

a probe generator operable to produce an ARP probe;

a response analyzer operable to analyze a response to an ARP probe and to determine whether the response to the ARP probe indicates that an IP address associated with the probing entity is a duplicate IP address; and

an active network detector operable to determine whether the system is connected to an active network, comprising:[[.]]

a network traffic analyzer that analyzes network traffic and determines whether the probing entity is connected to an active network;

a network pulse analyzer that analyzes one or more electrical signals received from network devices operably connected to the probing entity and that determines whether the probing entity is connected to an active network; and

a BPDU analyzer that analyzes one or more bridge protocol data units received by network devices operably connected to the probing entity and that determines whether the probing entity is connected to an active network.

16. (Cancelled)

17. (Currently amended) A computer readable medium storing computer executable components of a system for detecting and preventing the use of duplicate IP addresses, the system comprising:

a random time period generating component operable to produce a value representing a period of time that a probing entity should wait before invoking the processing of a probe generator component;

a probe generating component operable to produce an ARP probe;

a response analyzing component operable to analyze a response to an ARP probe and to determine whether the response to the ARP probe indicates that an IP address associated with the probing entity is a duplicate IP address; and

an active network detecting component operable to determine whether the system is connected to an active network that comprises:[[.]]

a network traffic analyzer that analyzes network traffic;

a network pulse analyzer that analyzes one or more electrical signals received from network devices operably connected to the probing entity; and

a BPDU analyzer that analyzes one or more bridge protocol data units received by network devices operably connected to the probing entity.

18. (Currently amended) A system for detecting and preventing the use of duplicate IP addresses comprising:

means for identifying a random period of time that should be waited before a probe generating means is activated;

means for generating an ARP probe;

means for distributing the ARP probe to one or more IP components;

means for interpreting a response to the ARP probe; [[and]]

means for determining whether a probing entity is connected to an active network;[[.]]

means for analyzing network traffic on a network interface associated with the probing entity;

means for analyzing electrical signals on hardware associated with the network with which the probing entity is to interact; and

means for analyzing BPDUs (Bridge Protocol Data Units) on a network device associated with the network with which the probing entity is to interact.